
Struktury dostępu i kryptosystemy oparte na krzywych eliptycznych

(Access structures and elliptic curve cryptosystems)

Autoreferat rozprawy doktorskiej

Jakub Derbisz

WSTĘP

Strukturę dostępu określamy jako trójkę $(\Sigma, \Gamma, \Lambda)$, w której Σ jest schematem podziału, Γ strukturą monotoniczną, zaś Λ strukturą anty-monotoniczną, w której struktura monotoniczna wyznacza zbiory uprzywilejowane, a struktura anty-monotoniczna tworzy zbiory nieuprzywilejowane. Innymi słowy, Σ jest metodą rozdzielania sekretu pomiędzy podmiotami pewnego zbioru, że zbiory zdolne do rekonstrukcji sekretu są właśnie zbiorami z monotonicznej struktury Γ , natomiast zbiory niezdolne do rekonstrukcji sekretu tworzą strukturę anty-monotoniczną Λ . Zadając tylko rodzinę zbiorów bazowych struktury monotonicznej Γ (to znaczy rodzinę minimalnych zbiorów generujących Γ), bądź tylko rodzinę zbiorów anty-bazowych (to znaczy rodzinę maksymalnych zbiorów generujących Λ) istnieje dokładnie jedna struktura dostępu modulo podziały sekretu Σ , zwane doskonałymi. Uzyskanie tego rezultatu pozwala nam opisywać struktury dostępu w terminach wyłącznie rodziny zbiorów bazowych lub anty-bazowych, mając w myślach pewien doskonały schemat podziału (pokazane jest w obydwu przypadkach, że istnieje

odpowiedni doskonały schemat podziału). To jeden z pierwszych, wstępnych rezultatów związanych z terminologią, której używamy i podstawowymi pojęciami w naszej pracy.

Zaczynając od odpowiednich definicji, mając u podstaw terminologię z teorii mnogości oraz rachunku prawdopodobieństwa, wyciągane wnioski mają charakter rozumowań związanych z teorią-mnogości, kombinatoryką oraz związanych z logiką. Używane są również metody z teorii baz Gröbnera. Chodzi tu o konstrukcje schematów dzielenia sekretu opartych na wielomianach wielu zmiennych. Pojawia się wykorzystanie teorii krzywych eliptycznych nad ciałem skończonym. Użyte przekształcenia dwuliniowe na krzywej eliptycznej to zmodyfikowany iloczyn Weila lub Tate’a Lichtenbauma. Wykorzystując grupę, w której Obliczeniowy Problem Diffie-Hellmana (CDHP) jest trudny, podczas gdy Decyzyjny Problem Diffie-Hellmana (DDHP) jest łatwy (ze względu na istnienie iloczynu dwuliniowego) zaproponowany jest schemat podpisu dedykowany dowolnej strukturze dostępu.

WYNIKI

W rozdziale przygotowawczym, z definicjami pojęć podstawowych, przedstawiono podstawowe podejścia do konstrukcji doskonałych schematów podziału dla ogólnej (monotonicznej) struktury dostępu. Konstrukcje te później, w następnym rozdziale, są uogólnione w sposób abstrakcyjny, w którym wykorzystywana jest funkcja spełniająca pewne teorio-mnogościowe warunki. Podane są dwa przykłady takich funkcji. Wspomniana generyczna funkcja ma w swojej dziedzinie pewną rodzinę zbiorów. Zbiorem wartości jest tutaj również pewna rodzina zbiorów. Spełnia ona takie warunki, które gwarantują iż podanie dowolnej jej realizacji owocuje powstaniem schematu dzielenia sekretu w dowolnej strukturze dostępu. W zastosowaniach chodzi o podawanie takich jej realizacji, by otrzymywane metody podziału sekretu były ‘naprawdę bezpieczne’. Ta ogólna metoda wraz z innymi prezentowanymi w pracy znajduje zastosowanie w ostatnim rozdziale, do konstrukcji schematu podpisu opartego na dowolnej strukturze dostępu.

W pracy zgodnie z leżącą u podstaw teorio-mnogościową oraz probabilistyczną terminologią, opisane są klasyczne schematy podziału sekretu. Opisany jest zatem między innymi schemat Shamira lub Blakley’a. W tej terminologii również przedstawiony został schemat podziału, który nazywamy rozszerzonym schematem Blakley’a i który to pochodzi z [6]. Opis schematów jest ujednolicony. Przedstawiamy go używając notacji opartej na wielomianach, które eksponujemy jako leżące u podstaw każdego ze schematów. W trzecim rozdziale rozszerzono wspomnianą notację podejmując próbę konstrukcji

schematów, które są w pewnym sensie bardziej ogólne niż dotychczas przedstawiane w literaturze (np. udziałami nie muszą być elementy ciała lecz mogą być wielomiany). Schematy te oparte są na wielomianach wielu zmiennych. Tu, nowe w literaturze podejście wykorzystuje elementy teorii baz Gröbnera. W pracy podane zostały przykłady realizacji takich schematów. Wprowadzona technika związana jest z algorytmem znajdowania minimalnego rozwiązania w Twierdzeniu Chińskim o Resztach (względem pewnego porządku na wielomianach) w pierścieniu wielomianów wielu zmiennych. Sam algorytm pochodzi z pracy [2]. Używamy go również aby znaleźć wszystkie rozwiązania CRT.

W prezentowanych schematach podziału opartych na powyższym podejściu, części dzielonego sekretu, który wstępnie jest wielomianem wielu zmiennych, są również takimi wielomianami. Z każdym podmiotem wiązany jest jego publiczny ideał z pierścienia wielomianów. Dzięki temu możliwym stało się podanie teoretycznej struktury, na której opierane mogą być schematy progowego dzielenia wielomianów wielu zmiennych. Prezentowane podejście pozwala również podać realizację (t, t) progowego schematu podziału sekretu opartego na wielomianie, którego stopień nie jest a priori znany.

Nowe spojrzenie na dzielenie sekretu umożliwia skonstruowanie schematu dzielenia wielomianu wielu zmiennych lub jego wartości w pewnym punkcie, dedykowane dla ogólnej struktury dostępu. W przeciwieństwie do teoretycznej, abstrakcyjnej konstrukcji schematu progowego, możliwa jest jego realizacja w pewnych strukturach dostępu wynikająca już z opisu w pracy. Podane są zalety takiej konstrukcji. Jedną z nich jest możliwość prostego przesyłania podmiotom ukrytych informacji, jeśli udziałami podmiotów są niestałe wielomiany. Przesyłającym jest w tym przypadku podmiot, który zaszyfrował w postaci udziałów pewien wielomian.

Część pracy, z rozdziału drugiego, związana jest z porównywaniem dwóch metod szyfrowania monotonicznej struktury dostępu. Pierwsza z nich jest dobrze znana. Była zaproponowana przez Benaloha i Leichterów w [4]. Jest ona związana z możliwościami szyfrowania monotonicznej struktury dostępu w oparciu o zadaną monotoniczną formułę logiczną. Druga z metod, o której była już mowa, to nasza rozszerzona metoda szyfrowania monotonicznej struktury dostępu w oparciu o podejście teorio-mnogościowe. Tam zaczynając od rodziny zbiorów bazowych lub anty-bazowych, przy użyciu pewnej funkcji otrzymuje się schemat podziału sekretu.

Pokazane są zależności między tymi dwiema metodami. Dowodzimy następujących twierdzeń, nazwanych tak raczej ze względu na ich wagę, nie zaś trudności w dowodzie:

Twierdzenie *Niech F będzie dowolną monotoniczną formułą logiczną określającą strukturę monotoniczną Γ . Przekształcając F do alternatywnej postaci normalnej i przeprowadzając redukcje tak, by żadna klauzula nie była zawarta jako zbiór literałów w innej, zbiory utworzone przez indeksy klauzul definiują bazę Γ .*

oraz twierdzenie dualne:

Twierdzenie *Niech F będzie dowolną monotoniczną formułą logiczną określającą strukturę monotoniczną Γ . Zapisując F w koniunkcyjnej postaci normalnej, która jest zredukowana tak, by nie było klauzul zawartych jako zbiory literałów w innych, zbiory tworzące anty-bazę konstruowane są poprzez wybranie klauzuli formuły i wypisanie wszystkich indeksów nie występujących w tej wybranej.*

Wyjaśnijmy, że monotoniczna formuła logiczna (taka składająca się z samych alternatyw i koniunkcji, bez negacji) zadaje strukturę monotoniczną na zbiorze podmiotów identyfikowanych z indeksami zmiennych występujących w formule (a_1, a_2 , itd.) w ten sposób, że zbiorami uprzywilejowanymi są te zbiory indeksów, dla których jeśli wstawimy w zmienne indeksowane elementami takiego zbioru wartość 1 w naszej formule, a w pozostałe miejsca 0, będzie to formuła prawdziwa. Przypomnijmy też, że bazą rodziny monotonicznej jest rodzina zbiorów minimalnych, tj. takich, w których żaden element rodziny monotonicznej nie jest już właściwie zawarty. Anty-bazą rodziny anty-monotonicznej Λ odpowiadającej Γ jest rodzina zbiorów maksymalnych w Λ (nic już dołożyć nie można).

W pracy prezentowane jest nowe ujęcie hierarchii. Jest to hierarchia w ogólnej strukturze dostępu. Wprowadzone pojęcie nie jest tym znanym z literatury odnoszącym się do hierarchicznych struktur dostępu. Wprowadzono raczej definicję hierarchii, której celem jest uchwycenie pewnych intuicji. Dążymy do koncepcji hierarchii w dowolnej monotonicznej strukturze dostępu tak, aby wyróżnić tych użytkowników, którzy intuicyjnie są bardziej pożądanymi przez adwersarza aby ich skorumpować. Nie skupiamy się jednak na teoretycznych aspektach związanych z taką definicją. Bierzemy raczej pod uwagę praktyczne sposoby dzielenia sekretu, które wiążą się z ukryciem miejsca zajmowanego przez podmiot w hierarchii intuicyjnie rozumianej w ten sposób. Tak postępując, dążymy na przykład do tego, aby adwersarz nie był w stanie rozróżnić między użytkownikiem, który jest 'najważniejszy', a takim który jest ważny najmniej. Prezentujemy odpowiedni schemat dzielenia sekretu pozwalający ukryć miejsca podmiotów w hierarchii. Zajmujemy

się szczegółowymi wynikami związanymi z bezpieczeństwem hierarchii i dowodzimy na przykład:

Twierdzenie *Dla rodziny zbiorów bazowych B monotonicznej struktury dostępu, takiej że żaden podmiot nie jest w stanie zrekonstruować sekretu sam, można zagwarantować, że zbiory S_i związane z podmiotami, w procesie rozdzielania udziałów opartym na podejściu z anty-bazą, nie są zawarte jeden w drugim.*

Zbiory S_i o których tutaj mowa pochodzą z naszej konstrukcji opartej na 'teorio-mnogościowej funkcji', której realizacje implikują schematy dzielenia sekretu. Tam $f(S_i)$ jest to zbiór, który jest udziałem i -tego podmiotu.

W pracy prezentowane są zastosowania w postaci konstrukcji opartych na krzywych eliptycznych nad ciałem skończonym, dedykowanych dla dowolnej monotonicznej struktury dostępu. Konstrukcje te oparte są na iloczynie dwuliniowym na krzywej eliptycznej nad ciałem skończonym. Iloczynami dwuliniowymi, które można tu wykorzystać, są na przykład zmodyfikowany iloczyn Weila lub zmodyfikowany iloczyn Tate'a-Lichtenbauma. Pokazano sposoby konstrukcji schematów podpisu dedykowanych dla monotonicznych struktur dostępu. Struktura monotoniczna w schemacie może być zaszyfrowana na różne rozpatrywane w pracy sposoby. Konstrukcje te mają swe fundamenty wspólne z podpisem grupowym bazującym na uogólnionym ciągu Asmutha-Blooma oraz algorytmie CRT-Orego, zaprezentowanym przez Pomykałę, i stanowią jego rozszerzenia w postaci możliwości szyfrowania innych struktur dostępu. Rozważanymi metodami szyfrowania struktury są:

- Metoda oparta na uogólnionym ciągu Asmutha-Blooma wykorzystująca algorytm CRT-Orego
- Metoda oparta o rozszerzony schemat Blakley'a, pochodzący od Brickella
- Metoda oparta o formuły logiczne wywodząca się od Benaloha i Leichter'a
- Metoda oparta o czyste teorio-mnogościowe podejście, która została wprowadzona w naszej pracy

PRZYKŁADOWE REZULTATY

Hierarchia w dowolnej monotonicznej strukturze dostępu

Przez X oznaczamy zbiór podmiotów.

Definicja z [14], która ujmuje wszystkie dotychczas rozważane w literaturze opisy struktur hierarchicznych jest następująca.

Definicja Niech Γ będzie monotoniczną rodziną zbiorów. Mówimy, że podmiot $P_1 \in X$ jest wyżej w hierarchii od podmiotu $P_2 \in X$, jeżeli $A \cup \{P_1\} \in \Gamma$ dla każdego podzbioru $A \subseteq X \setminus \{P_1, P_2\}$ takiego, że $A \cup \{P_2\} \in \Gamma$. Struktura dostępu jest hierarchiczna jeśli wszystkie podmioty są hierarchicznie powiązane.

Jak widzimy rozważa się w niej pewne szczególne struktury, zwane hierarchicznymi. Prezentowany przez nas opis wywodzi się ze spostrzeżenia, że w każdej monotonicznej rodzinie możemy spróbować wskazać podmiot, który jest najbardziej, od strony adwersarza, pożądanym do korupcji. Proponujemy zatem następującą definicję:

Definicja Miejsce podmiotu w hierarchii zależy od liczby zbiorów uprzywilejowanych w X , które ten podmiot zawierają. Tak więc podmiot $P_1 \in X$ jest wyżej w hierarchii od podmiotu $P_2 \in X$, jeśli moc rodziny $\mathbf{F}_1 = \{A \in \Gamma : P_1 \in A\}$ jest nie mniejsza od mocy rodziny $\mathbf{F}_2 = \{A \in \Gamma : P_2 \in A\}$.

Definicja dotyczy zatem dowolnej monotonicznej struktury dostępu. W pracy jednak traktujemy ją intuicyjnie i koncentrujemy się na takiej konstrukcji schematu dzielenia sekretu, która pozwala ukryć powiązania w hierarchii. Żądamy, by z liczby udziałów, w pewnej metodzie dzielenia sekretu opartej na rodzinie zbiorów anty-bazowych nie można było wywnioskować miejsca, które podmiot zajmuje w hierarchii. Zazwyczaj bowiem, z podmiotami najwyższymi w hierarchii, stowarzyszonych jest najwięcej rozdzielanych elementów, a z najniższymi najmniej. Celem jest by niemożliwym było rozróżnienie między podmiotami najwyższymi i najniższymi, po uzyskaniu ich udziałów przez adwersarza. Rozważana konstrukcja opiera się na metodzie z funkcją o charakterze teorio-mnogościowym. Chodzi nam tu o pewne przekształcenie operujące na zbiorach i spełniające z nimi związane warunki, które umożliwia konstrukcję schematów dzielenia sekretu. Bierzemy pod uwagę najmniejszą wspólną wielokrotność odpowiednich liczb.

Przykład

Rozważmy zbiór podmiotów $X = \{P_1, P_2, P_3, P_4\}$ oraz rodzinę zbiorów bazowych

$\mathbf{B} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3\}, \{P_1, P_4\}\}$.

Rodzina zbiorów maksymalnych nieuprzywilejowanych (anty-baza) to

$\mathbf{N} = \{\{P_1\}, \{P_2, P_4\}, \{P_3, P_4\}\}$.

Podmiotem najbardziej uprzywilejowanym (najwyżej w hierarchii) jest P_1 . Może on zrekonstruować sekret współpracując z dowolnym innym podmiotem. Liczba uprzywilejowanych podzbiorów które zawierają P_1 jest największa (jest ich 7, podczas gdy dla P_2 oraz P_3 jest ich 6, dla P_4 jest ich 5). Najmniej uprzywilejowanym podmiotem jest P_4 gdyż zrekonstruować on sekret może wyłącznie z P_1 . Liczba uprzywilejowanych podzbiorów zawierających P_4 jest najmniejsza. W metodzie dzielenia sekretu z P_1 związane będą dwie liczby, zaś z P_4 tylko jedna. W naszym podejściu chcemy ukryć tę zależność.

Wielowymiarowe rozszerzenia schematów podziału sekretu

Zaprezentujemy spojrzenie z pracy na dobrze znany schemat dzielenia sekretu Shamira. Korzysta się tutaj z algorytmu wyznaczającego rozwiązanie Twierdzenia Chińskiego o Resztach w pierścieniu wielomianów wielu zmiennych. Podajmy najpierw odpowiednie twierdzenie. Wywodzi się ono z pracy [2].

Niech $R = K[X_1, \dots, X_l]$, gdzie K jest ciałem.

Twierdzenie Dla ideałów I_1, \dots, I_m pierścienia R oraz wielomianów $f_1, \dots, f_m \in R$, przecięcie zbiorów $\bigcap_{j=1}^m (f_j + I_j)$, jeżeli niepuste, równe jest $f' + \bigcap_{j=1}^m I_j$, gdzie konstruowalny $f' \in R$ jest minimalny w $\bigcap_{j=1}^m (f_j + I_j)$ pod względem praporządku na wielomianach R indukowanego z porządku na jednomianach monicznych w R .

Pisząc tutaj konstruowalne, mamy na myśli, że odpowiednie algorytmy na konstrukcję wspomnianych elementów znaleźć możemy w pracy [2]. Porządek na jednomianach, o którym mowa w twierdzeniu to tak zwany dopuszczalny porządek na jednomianach monicznych znany w teorii baz Gröbnera. Możemy rozważyć na przykład porządek zwany stopniem leksykograficznym. Indukuje on praporządek (relację zwrotną i przechodnią, bez antysymetryczności) na wielomianach przez porównywanie, dla dwóch danych wielomianów, ich największych jednomianów (pomijamy współczynniki), jeśli równe to porównywaniu następnych jednomianów itd.

Podamy jak w tych terminach wygląda zapisanie schematu progowego (t, n) Shamira.

Chociaż w schemacie Shamira rozważa się wielomian jednej zmiennej, podobne elementy konstrukcji przenoszą się na wyższe wymiary.

Niech $K = \mathbb{F}_q$ odpowiednio duże.

Niech $f = f(X) = a_0 + a_1X + \dots + a_{t-1}X^{t-1} \in K[X]$ będzie wybrany losowo (losując współczynniki). Wybieramy dla podmiotów ze zbioru $\{P_1, \dots, P_n\}$ (dla $t \leq n$) ich tożsamości. Powiedzmy, że będą to niezerowe, różne elementy ciała $c_1, c_2, \dots, c_n \in K$. Niech $f(c_i) = r_i$ dla $i = 1, \dots, n$ będą udziałami podmiotów. Skoro $f(c_i) - r_i = 0$ to $(X - c_i) | (f(X) - r_i)$ co w języku ideałów można zapisać jako: $f \in r_i + (X - c_i)$. Zatem użytkownik posiada $r_i + (X - c_i)$. Załóżmy, że t użytkowników zgromadziło się by zrekonstruować sekret, tutaj powiedzmy zrekonstruować wielomian. Bez straty ogólności powiedzmy, że są to użytkownicy o tożsamościach c_1, \dots, c_t . Zatem w twierdzeniu rozważany będzie zbiór stałych wielomianów r_1, \dots, r_t oraz ideałów $(X - c_1), \dots, (X - c_t)$. Porządek będzie indukowany z porządku stopnia-leksykograficznego na jednomianach. Uogólniony algorytm CRT znajduje takie f' , że

$$f' + \bigcap_{j=1}^t (X - c_j) = \bigcap_{j=1}^t (r_j + (X - c_j)) .$$

Mamy też $\bigcap_{j=1}^t (X - c_j) = (\prod_{j=1}^t (X - c_j))$. Skoro f' jest minimalny w $\bigcap_{j=1}^t (r_j + (X - c_j))$ oraz $f \in \bigcap_{j=1}^t (r_j + (X - c_j))$ więc $\deg(f') \leq \deg(f) \leq t - 1$.

Mamy więc $f \in f' + (\prod_{j=1}^t (X - c_j))$, skąd $f = f' + h \prod_{j=1}^t (X - c_j)$, dla pewnego wielomianu h . Czyli $f - f' = h \prod_{j=1}^t (X - c_j)$, a ze względu na stopień $h = 0$, zatem wielomian f' , który grupa t użytkowników zrekonstruowała jest tym, o który chodzi.

Powyższa notacja jest odpowiednia do uogólnienia podziału sekretu na przypadek wielomianu wielu zmiennych i ogólnych struktur dostępu.

Konstrukcje na krzywych eliptycznych

W rozwinięciach schematu podpisu grupowego, zaproponowanego przez Pomykałę, korzysta się z własności dwuliniowości iloczynu Weila i Tate'a-Lichtenbauma. Rozpatrywane są iloczyny te po odpowiednich modyfikacjach, tak żeby na przykład zmodyfikowany iloczyn Weila mógł być nietrywialny na parze tych samych punktów, zaś w podobnym sensie niezdegenerowany iloczyn Tate'a-Lichtenbauma miał wartości nie w przestrzeni warstw lecz grupie pierwiastków z jedności. Są to standardowe konstrukcje, na których opiera się rozważany schemat podpisu. Wykorzystujemy tu Grupy Diffie-

Hellmana z luką obliczeniową. Są to grupy, w których CDHP jest trudny, a DDHP łatwy. Takich grup należy szukać wśród podgrup n -torsyjnych punktów na krzywych supersingularnych [9]. Schemat samej konstrukcji podpisu polega na takim utworzeniu klucza publicznego S dla grupy, aby możliwym było podzielenie go na części (udziały) dla użytkowników w ten sposób, by grupy uprzywilejowane ze swoich udziałów, korzystając z własności dwuliniowości iloczynu mogły składać zagregowane podpisy cyfrowe pod wiadomościami tak, by przy użyciu klucza publicznego grupy można je było zweryfikować. W konstrukcjach korzysta się z klucza prywatnego s grupy, a mnożąc go przez zadany publicznie punkt krzywej eliptycznej Q otrzymuje się klucz publiczny grupy: $S = sQ$. Podpisu w zastosowanych metodach każdy użytkownik dokonuje mnożąc części s związane z przydzielonym udziałem przez punkt krzywej eliptycznej odpowiadający aktualnie podpisywanej wiadomości. Podpisy poszczególnych użytkowników następnie łączy się w podpis grupowy. Chodzi o to, by tworząc podpis grupowy operować tylko na podpisach częściowych poszczególnych użytkowników, nie zaś na wiedzy o ich udziałach.

W metodzie korzystającej z uogólnionego ciągu Asmutha-Blooma (q, p_1, \dots, p_n) związanego zadaną strukturą monotoniczną Γ (który to ciąg dla zadanej Γ może być wyznaczony metodą opratą na podejściu ze zbiorami anty-bazowymi) rekonstrukcja bazuje na algorytmie CRT-Orego. Szuka się tam rozwiązania układu kongruencji, w którym moduły nie muszą być względnie pierwsze. W metodzie tej konstruuje się odpowiedni, losowy sekretny klucz grupowy s , który później dzieli się w postaci udziałów jak w Chińskim Twierdzeniu o Resztach, z modułami p_1, \dots, p_n pochodzącymi z ciągu Asmutha-Blooma.

W metodzie podpisu opartej na rozszerzonym schemacie Blakley'a pochodzącej od Brickella działamy w przestrzeni liniowej \mathbb{F}_q^t , skąd też wybierane są tożsamości użytkowników (wektory \mathbf{v}_i , które są im przypisane). Grupowym kluczem prywatnym jest $s = \mathbf{a} \cdot \mathbf{v}$, gdzie \mathbf{a} wybrane jest losowo. Udziałami użytkowników są $s_i = \mathbf{a} \cdot \mathbf{v}_i$. Zbiory uprzywilejowane Γ względem wybranego wektora $\mathbf{v} \in \mathbb{F}_q^t$ w tej metodzie budują ci użytkownicy, których odpowiadające wektory rozpinają przestrzeń zawierającą \mathbf{v} (tutaj tak zadawana struktura nie jest zupełnie dowolną monotoniczną strukturą dostępu). Podpis można utworzyć dzięki temu, że grupa uprzywilejowana znając przypisane wektory tożsamości które są publiczne, może znaleźć współczynniki z ciała takie, że $\sum c_i \mathbf{v}_i = \mathbf{v}$. Dzięki tym współczynnikom użytkownicy bezpiecznie łączą swoje poszczególne podpisy w podpis grupowy.

W metodzie opartej na formułach logicznych korzysta się z addytywnego podziału sekretu względem formuły logicznej, zaproponowanym przez Benaloha i Leichter. Gru-

powy klucz prywatny losowany jest jako element $s \in \mathbb{Z}_q$ i rozdzielany w postaci udziałów zgodnie z metodą opartą na formule logicznej. W rezultacie użytkownicy tworzą grupę uprzywilejowaną, wśród swoich udziałów znajdują takie, które sumują się do s . Użytkownik składający podpis w ramach tej grupy, dla weryfikacji podaje również zbiór indeksów odpowiadających jego częściom udziału, które wchodziły w skład s (z każdym indeksem i związany jest publicznie znany punkt s_iQ). Podpisy poszczególnych użytkowników sumuje się otrzymując podpis grupowy.

Dla podpisu opartego na wprowadzonej w pracy metodzie korzystającej z przekształcenia f , które z rodziny zbiorów prowadzi w rodzinę zbiorów, zadane zostają dwa działania $*$ oraz \boxplus tak, by dla rodziny \mathbf{F} będącej zbiorem wartości f oraz stosowanej podgrupy G na krzywej eliptycznej z dziedziny iloczynu dwuliniowego mieć:

$$* : \mathbf{F} \times G \rightarrow G$$

oraz

$$\boxplus : G \times G \rightarrow G .$$

Spełniają one warunki, które w połączeniu z konstrukcją struktury dostępu opartą na funkcji f pozwalają na realizację schematu podpisu grupowego. Przekształcenie te zadajemy po to, by możliwe były działania algebraiczne na udziałach podmiotów, które są tutaj zbiorami (są to zbiory $f(S_i)$ o których wspominaliśmy w ramach bezpieczeństwa w hierarchii).

W podobny sposób w jaki skonstruowano schemat podpisu grupowego dedykowanego dowolnej strukturze dostępu, dla metod zadawania struktur dostępu użytych powyżej, można skonstruować grupowy schemat deszyfrowania wiadomości w dowolnej strukturze.

LITERATURA

- [1] C. Asmuth, J. Bloom, *A modular approach to key safeguarding*, IEEE Trans. on Information Theory, IT-29(2):208-211, 1983.
- [2] T. Becker, V. Weispfenning, *The Chinese remainder problem, multivariate interpolation, and Gröbner bases*, Proc. ISSAC'91, Bonn, ACM Press, 64–69, New York 1991.
- [3] T. Becker, V. Weispfenning, *Gröbner Bases: A Computational Approach to Commutative Algebra*, Springer-Verlag, 1993.

- [4] J. Benaloh and J. Leichter, *Generalized secret sharing and monotone functions*, Advances in Cryptology - CRYPTO '88.
- [5] G. Blakley, *Safeguarding cryptographic keys*, Proceedings of the National Computer Conference 48: 313–317, 1979
- [6] E.F. Brickell, *Some ideal secret sharing schemes*, J. Combin. Math. Combin. Comput. 9, 105–113, 1989.
- [7] D. Boneh, M. Franklin, *Identity-based encryption from the Weil pairing*, Advances in cryptology, Crypto 2001 (Santa Barbara, CA), volume 2139 of Lecture Notes in Comput. Sci., 213–229, Springer-Verlag, Berlin 2001.
- [8] B. Buchberger, *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory*, N. K. Bose ed. Recent trends in Multidimensional System theory. Dordrecht: Reidel, 184–232, 1985.
- [9] J.C. Cha, J.H. Cheon, *An identity-based signature from gap Diffie-Hellman groups*, Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, Springer, Heidelberg, 18–30 2002.
- [10] J. Derbisz, *Methods of encrypting monotonic access structures*, Annales Universitatis Mariae Curie-Skłodowska Sectio AI Informatica XI, 2, 49–60, 2011.
- [11] J. Derbisz, J. Pomykała, *Pairing based group cryptosystem with general access structures*, Cyberprzestępczość i ochrona informacji, 329–348, WSM, Warszawa, 2012.
- [12] J. Derbisz, J. Pomykała, *Uogólnione rozdzielanie sekretu w systemach rozproszonych*, Cyberprzestępczość i ochrona informacji, 311–328, WSM, Warszawa, 2012.
- [13] T. Elgamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory, IT-31(4):469–472, 1985.
- [14] O. Farràs, C. Padró, *Ideal hierarchical secret sharing schemes*, Seventh IACR Theory of Cryptography Conference, TCC 2010, Lecture Notes in Comput. Sci., vol. 5978, 219–236, 2010.
- [15] S. D. Galbraith, *Pairings, Advances in elliptic curve cryptography*, London Math. Soc. Lecture Note Ser., vol. 317, Cambridge University Press, Cambridge, 183–213, 2005.
- [16] M. Ito, A. Saito, T. Nishizeki, *Secret Sharing Scheme Realizing General Access Structure*, Proc. Glob. Com, 1987.
- [17] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation, 48, 203–209, 1987.
- [18] V. S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology-CRYPTO '85, Lecture Notes in Computer Science, Springer-Verlag, 218, 417–426, 1986.
- [19] V. Miller, *The Weil pairing and its efficient calculation*, J. Cryptology, 17(4):235–261, 2004.
- [20] O. Ore, *The general Chinese remainder theorem*, American Mathematical Monthly, 59:365–370, 1952.
- [21] A. Shamir, *How to share a secret*, Communications of the ACM 22 (11): 612–613, 1979.